SENIOR 2012 Medium - Algebra 1

Titolo nota 04/09/2012

Polinomi
→ Riepilogo livello Basic
→ Fattorizzazione
→ Esercizi

Polinomio: $a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ $\quad a_i \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ = classi di resto modulo p

field

I coefficienti stanno in un ANELLO = ambiente in cui posso fare $+, -, \cdot$

$\boxed{\text{PRINCIPIO DI IDENTITÀ DEI POLINOMI}}$ Dati $P(x)$ e $Q(x)$

Sono fatti equivalenti (se l'ambiente ha infiniti elementi)

1. hanno gli stessi coeff.
2. $P(x) = Q(x)$ per ogni $x \in$ ambiente

[Oss. Se |ambiente| < +∞, allora NON vale [Ex]]

Oss. In $\mathbb{F}_p$ non c'è l'equivalenza $P(x) = 0$ $\quad Q(x) = x^p - x = 0$ per ogni $x \in \mathbb{F}_p$ (FLT)

Di cosa è figlia l'equivalenza?

Se un polinomio ha grado n si annulla per $n+1$ valori distinti di x, allora il polinomio è nullo, cioè ha tutti coeff. $= 0$.

$P(x) - Q(x)$ se si annulla in $n+1$ valori, dove n è il suo grado, allora tutti coeff. $= 0$, allora coeff. $P(x)$ = coeff. di $Q(x)$

Ruffini o fattorizzazione Se α è radice di $P(x)$, cioè $P(\alpha) = 0$, allora

$P(x) = (x-\alpha)\, Q(x)$ $\quad$ cioè $P(x)$ è divisibile per $(x-\alpha)$

Deriva dalla divisione Euclidea: dati $A(x)$ e $B(x)$, esistono $Q(x)$ ed $R(x)$ t.c.

$$A(x) = B(x) \cdot Q(x) + R(x) \quad \text{e} \quad \deg(R(x)) < \deg(B(x))$$

Divido $A(x)$ dato per $B(x) = x-\alpha$

$$A(x) = (x-\alpha)\cdot Q(x) + R(x)$$
$$= (x-\alpha)\cdot Q(x) + \underset{\substack{\uparrow \\ \text{Numero}}}{c}$$

Metto $x=\alpha$ $\quad 0 = A(\alpha) = 0 + c \Rightarrow c = 0.$

Se $P(x)$ ha grado n e ha n radici distinte $\lambda_1, \dots, \lambda_n$, allora

$$P(x) = c\,(x-\lambda_1)(x-\lambda_2)\cdot\ldots\cdot(x-\lambda_n)$$

Non può annullarsi per un altro $x \neq \lambda_1, \lambda_2, \dots, \lambda_n$

Di cosa è figlia la divisione Euclidea? Del fatto che l'insieme dei coefficienti è un CAMPO (cioè posso dividere i coeff.)

Oss. Si può sempre dividere (anche non nei campi) se il divisore è MONICO. Questo basta per dimostrare Ruffini.

BEZOUT Sugli interi Dati a e b coprimi, esistono m ed n t.c.

$$ma + nb = 1$$

Sui polinomi: $P(x)$ e $Q(x)$ sono coprimi $\Leftrightarrow$ non esiste un polinomio di grado ≥ 1 che li divide entrambi

Bezout: dati $P(x)$ e $Q(x)$ coprimi, esistono $M(x)$ ed $N(x)$ t.c.

$$M(x)\,P(x) + N(x)\cdot Q(x) = 1$$

QUESTO VALE NEI CAMPI (DOVE POSSO FARE LA DIVISIONE)

Cosa si salva in $\mathbb{Z}$? $\quad A(x) \in \mathbb{Z}[x] \quad B(x) \in \underbrace{\mathbb{Z}[x]}_{\text{pol. a coeff. in } \mathbb{Z}}$

Pensandoli in $\mathbb{Q}[x]$ ottengo $M(x), N(x) \in \mathbb{Q}[x]$ per cui vale BEZOUT

$$M(x)\cdot A(x) + N(x)\cdot B(x) = 1$$

Moltiplicando per il denominatore comune ottengo

$$\bar{M}(x)\cdot A(x) + \bar{N}(x)\cdot B(x) = d \qquad \bar{M}(x) \text{ e } \bar{N}(x) \in \mathbb{Z}[x]$$

Ricaduta aritmetica Siano $A(x)$ e $B(x)$ due polinomi senza fattori in comune in $\mathbb{Z}[x]$

Sia $m \in \mathbb{N}$. Allora $MCD(A(m), B(m))$ deve per forza dividere d

Esempio $A(x) = x^2+x+1$ $\quad B(x) = x-1$

$$\begin{array}{l|l} x^2+x+1 & x-1 \\ -x^2+x & x+2 \\ \hline \quad 2x+1 & \\ \quad -2x+2 & \\ \hline \quad\quad 3 & \end{array}$$

$$x^2+x+1 = (x-1)(x+2)+3$$

$$\underbrace{1}_{\overline{M}(x)}\underbrace{(x^2+x+1)}_{A(x)} - \underbrace{(x-1)}_{B(x)}\underbrace{(x+2)}_{\overline{N}(x)} = 3$$

Quali sono i primi che possono dividere contemporaneamente $x-1$ e x^2+x+1 ? Solo $p=3$!

Oss. Nel principio di identità basta che $P(x) = Q(x)$ per un numero di $x = \max\{\deg(P), \deg(Q)\}+1$

— o — o —

Siano $x_1, \dots, x_n, x_{n+1} \in$ ambiente distinti, Siano $y_1, \dots, y_n, y_{n+1} \in$ ambiente anche non distinti

Cerco $P(x)$ di grado $\leq n$ t.c. $P(x_i) = y_i \quad \forall i = 1, \dots, n+1$

Risposta affermativa $\Leftrightarrow$ ambiente è un campo

1ª DIM Risolvere il problema quando gli y_i sono tutti 0 tranne uno che vale 1. Sia $P_i(x)$ la soluzione con $P_i(x_i) = 1$ e $P_i(x_j) = 0$ $j \neq i$

Allora la soluzione generale è $P(x) = y_1 P_1(x) + \dots + y_{n+1} P_{n+1}(x)$

2ª DIM Impongo il sistema sui coefficienti. $P(x) = a_0 + a_1 x + \dots + a_n x^n$

$P(x_1) = y_1 \qquad a_0 + a_1 x_1 + \dots + a_n x_1^n = y_1$

$P(x_2) = y_2 \qquad a_0 + a_1 x_2 + \dots + a_n x_2^n = y_2$

$\vdots$

Ho $(n+1)$ incognite $a_0, a_1, \dots, a_n$ e $(n+1)$ equazioni

Teorema Un sistema lineare quadrato ha soluzione unica per ogni termine noto $(y_1, y_2, ..., y_{n+1})$ $\iff$ matrice dei coeff. ha det. $\neq 0$.

In questo caso

$$\text{Matrice} = \begin{matrix} 1 & x_1 & x_1^2 & x_1^3 & \dots & x_1^n \\ 1 & x_2 & x_2^2 & x_2^3 & \dots & x_2^n \\ \vdots \\ 1 & x_{n+1} & x_{n+1}^2 & & \dots & x_{n+1}^n \end{matrix}$$

VANDERMONDE

Questa matrice ha det $\neq 0 \iff$ gli x_i sono tutti diversi.

—o—o—

Congruenze tra polinomi Figlie della divisione con resto

Esercizio $P(x) = x^{2012} + 3x^{1943} + 7x^3 - 12$

$P(x)$ diviso (x^2+1) Trovare il resto

1° modo: fare la divisione...

2° modo: $P(x) = (x^2+1)\,Q(x) + ax + b$ in $\mathbb{Z}[x]$

Metto $x = i$ $\quad \boxed{P(i)} = ai + b$

Metto $x = -i$ $\quad \boxed{P(-i)} = a(-i) + b$

$\left.\begin{matrix} \\ \end{matrix}\right\}$ sistema nelle incognite a e b

si calcolano

3° modo Congruenze modulo x^2+1

$x^2 \equiv -1 \pmod{x^2+1}$

$x^{4k} \equiv 1 \pmod{x^2+1}$

$x^3 \equiv -x \pmod{x^2+1}$

$x^{2012} \equiv 1 \pmod{x^2+1}$

$x^{1943} \equiv x^{1940} \cdot x^3 \equiv x^3 \equiv -x \pmod{x^2+1}$

$P(x) \equiv 1 - 3x - 7x - 12 = -10x - 11 = R(x)$

$\mathbb{Z}[x,y] = (\mathbb{Z}[x])[y]$

I polinomi in x e y sono polinomi in y con coeff. che sono polinomi in x.

<u>Esercizio</u> Sia $P(x,y) \in \mathbb{Z}[x,y]$

Supponiamo che si annulli in infiniti p.ti della parabola $y=2x^2$

Allora si annulla in tutti i p.ti della parabola e

$$P(x,y) = (y-2x^2)\, Q(x,y)$$

<u>Dim</u>: divido $P(x,y)$ per $y-2x^2$. Posso perché è monico in y !!!

$$P(x,y) = Q(x,y)(y-2x^2) + \underbrace{R(x,y)}_{\text{di grado 0 in } y}$$

$$= Q(x,y)(y-2x^2) + R(x)$$

Sostituisco i p.ti della parabola per cui $P(x,y)$ si annulla

$0 = P(x_i, 2x_i^2) = 0 + R(x_i) \Rightarrow R$ si annulla ∞ volte $\Rightarrow R \equiv 0.$

<u>Oss.</u> $R(x) = P(x, 2x^2)$ ← può avere grado fino al doppio di P

Di sicuro bastano $2\deg(P)+1$ annullamenti sulla parabola.

—o—o—

FATTORIZZAZIONE

1 - Radici razionali
2 - Modulo p
3 - EISENSTEIN
4 - Eisenstein ∞

Problema generale: dato $P(x) \in \mathbb{Z}[x]$ capire se si può fattorizzare

Radici razionali Se $P(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ e $x = \frac{p}{q}$ è una radice razionale con $(p,q) = 1$

Allora $q \mid a_n$ e $p \mid a_0$

Dim.: sostituisco $a_0 + a_1 \frac{p}{q} + a_2 \frac{p^2}{q^2} + \dots + a_n \frac{p^n}{q^n}$

$$= \frac{a_0 q^n + a_1 p q^{n-1} + \dots + a_{n-1} p^{n-1} q + a_n p^n}{q^n} = 0$$

Il 1° multiplo di p: $p \mid a_0 q^n$, ma $(p,q)=1 \Rightarrow p \mid a_0$

$q \mid a_n p^n$, ma $(p,q)=1 \Rightarrow q \mid a_n$

Corollario $P(x) \in \mathbb{Z}[x]$ ha fatto di 1° grado $(qx+p) \Leftrightarrow$ ha radice razionale e si decide in numero finito di tentativi.

— o — o —

(2) Sia $A(x) \in \mathbb{Z}[x]$, sia p primo. Ad $A(x)$ posso associare $\bar{A}(x) \in \mathbb{F}_p[x]$ (basta prendere tutti i coeff. mod p)

Se $A(x) = B(x) \cdot C(x)$, allora $\bar{A}(x) = \bar{B}(x) \cdot \bar{C}(x)$

Conseguenza: se esiste almeno un primo p per cui $\bar{A}(x)$ è irriducibile, allora non lo era nemmeno $A(x)$

Non è semplice capire se un polinomio in $\mathbb{F}_p[x]$ si fattorizza o no, ma almeno è un numero finito di tentativi (basso se p e grado piccoli)

— o — o —

③ Eisenstein Se esiste p primo tale che

$p \nmid a_n$, $p \mid a_i \quad \forall i = 0, 1, \dots, n-1$, $p^2 \nmid a_0$

Allora $P(x)$ è irriducibile

$\boxed{\text{DIM 1}}$ Supponiamo $P(x) = B(x) \cdot C(x)$

$B(x) = b_0 + b_1 x + \dots + b_k x^k$

$C(x) = c_0 + c_1 x + \dots + c_h x^h$

Coefficienti del prodotto

$a_0 = b_0 c_0$ uno solo dei 2 è div. per p : wlog $p \mid b_0$, $p \nmid c_0$

$a_1 = b_1 c_0 + \underbrace{b_0 c_1}_{p}$ quindi $p \mid b_1 c_0$, ma $p \nmid c_0$, quindi $p \mid b_1$

$\uparrow p$

$a_2 = b_2 c_0 + b_1 c_1 + b_0 c_2$ $\Rightarrow$ $p \mid b_2 c_0$, ... $\Rightarrow$ $p \mid b_2$

$\uparrow p \qquad \uparrow p \qquad \uparrow p$

Quando finisce? Solo con a_n, quindi con a_{n-1} è ancora vera

$a_{n-1} = b_{n-1} c_0 + b_{n-2} c_1 + \dots + b_1 c_{n-2} + b_0 c_{n-1}$ quindi $p \mid b_{n-1}$

$\uparrow p \qquad \uparrow p \qquad \uparrow p \qquad \uparrow p$

↗ se $\deg(B) \leq n-1$, allora tutti i coeff. di B sono multipli di p, ma allora anche tutti i coeff. di $P(x)$ sarebbero multipli di p (ASSURDO)

↘ se $\deg(B) = n$, allora $\deg(C) = 0$ e non si scompone.

$\boxed{\text{DIM 2}}$ Riduco il polinomio modulo p $\overline{P}(x) = a_n x^n$

Supponiamo $P(x) = A(x) \cdot B(x) \Rightarrow a_n x^n = \overline{A}(x) \cdot \overline{B}(x)$

$= a_n x^k \cdot x^{n-k}$

Questo dice che $A(x)$ e $B(x)$ hanno tutti i coeff. multipli di p tranne quello di grado max $\Rightarrow$ hanno termini noti multipli di p $\Rightarrow$ $P(x)$ ha termine noto multiplo di p^2.

Questo non funziona solo se termine noto = termine di grado max

Se $\overline{A}(x) = x^k \Rightarrow A(x) = x^k + p\,Q(x)$

Lemma di GAUSS Se $A(x) \in \mathbb{Z}[x]$ si fattorizza in $\mathbb{Q}[x]$, allora
" " " $\mathbb{Z}[x]$.

Esempio $x^2-1 = \left(\frac{1}{2}x+\frac{1}{2}\right)(2x-2)$ Esempio di fattorizzazione in $\mathbb{Q}[x]$ ma non in $\mathbb{Z}[x]$.

Lemma Dato $P(x) \in \mathbb{Z}[x]$ si definisce $MCDC(P(x)) = MCD(a_0, \dots, a_n)$.
Allora $MCDC(A(x) \cdot B(x)) = MCDC(A(x)) \cdot MCDC(B(x))$

Dim È banale che RHS | LHS
Devo dimostrare che LHS | RHS
wlog posso supporre $MCDC(A(x)) = 1$ $MCDC(B(x)) = 1$.
[convincersene per esercizio]
Voglio dimostrare che LHS = 1. Supponiamo per assurdo che non lo sia
cioè tutti i coeff. di $A(x) \cdot B(x)$ sono multipli di un certo primo p.
Per ipotesi sappiamo che $A(x)$ ha coeff. non multiplo di p
$B(x)$ ha coeff. " " " "

TRUCCO: Sia $a_k x^k$ il termine di $A(x)$ con coeff. non multiplo di p e grado + basso
Sia $b_h x^h$ la stessa cosa in $B(x)$
Coeff. di x^{k+h} in $A(x) \cdot B(x)$ è

$$\underbrace{a_0 b_{k+h} + a_1 b_{k+h-1} + \dots}_{p \text{ ci sta per colpa di } a} + \underbrace{a_k b_h}_{p \text{ non ci sta}} + \underbrace{a_{k+1} b_{h-1} + \dots + a_{k+h} b_0}_{p \text{ ci sta per colpa di } b}$$

$\boxed{\text{DIM LEMMA GAUSS}}$ Fattorizzo $A(x)$ in $\mathbb{Q}[x]$

$$A(x) = B(x) \cdot C(x) = \frac{\bar{B}(x)}{m} \cdot \frac{\bar{C}(x)}{n}$$ con $\bar{B}(x), \bar{C}(x) \in \mathbb{Z}[x]$

$\Rightarrow m \cdot n \cdot A(x) = \bar{B}(x) \cdot \bar{C}(x)$ Supponiamo wlog che $MCDC(A) = 1$
(convincersi che si può)

$$m \cdot n = MCDC(mn\,A(x)) = MCDC(\bar{B}(x) \cdot \bar{C}(x)) \underset{\text{Lemma prima}}{=} MCDC(\bar{B}(x)) \cdot MCDC(\bar{C}(x))$$

$$A(x) = \frac{\bar{B}(x)}{m} \cdot \frac{\bar{C}(x)}{n} = \frac{\bar{B}(x) \cdot \bar{C}(x)}{MCDC(\bar{B}) \cdot MCDC(\bar{C})} = \underbrace{\frac{\bar{B}(x)}{MCDC(\bar{B})}}_{\text{in } \mathbb{Z}[x]} \underbrace{\frac{\bar{C}(x)}{MCDC(\bar{C})}}_{\text{in } \mathbb{Z}[x]}$$

Eisenstein ∞ $A(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \in \mathbb{Z}[x]$

a_0 è primo $|a_0| > |a_1| + |a_2| + \dots + |a_n|$

Allora $A(x)$ è irriducibile

Dim. Supponiamo $A(x) = B(x) \cdot C(x)$. Wlog $b_0 = \pm 1$ $c_0 = \pm p$ primo

Ma $b_0 = \pm$ prodotto radici complesse di $B(x)$. Ma allora $B(x)$ ha una radice complessa z t.c. $|z| \leq 1$. Ma allora

$$a_0 = \underbrace{\sum_{i=0}^{n} a_i z^i}_{A(z) = B(z) \cdot C(z) = 0} - \sum_{i=1}^{n} a_i z^i \qquad a_0 = -\sum_{i=1}^{n} a_i z^i$$

$B(z) = 0$

faccio i moduli:

$$|a_0| = \left| \sum_{i=1}^{n} a_i z^i \right| \leq \sum_{i=1}^{n} |a_i| \cdot |z|^i \leq \sum_{i=1} |a_i|$$

ma per ipotesi ho supposto il contrario.

L'assurdo è nato dall'aver supposto $\deg(B) \geq 1$, altrimenti non potevo parlare delle sue radici.

— o — o —

INPUT : LEZIONE A1 MEDIUM 2011 → parecchi esempi interessanti

$\boxed{\text{IMO 1993-1}}$ $n>1$ $x^n+5x^{n-1}+3 = A(x)$ Dim. irriducibile in $\mathbb{Z}[x]$

Supponiamo $A(x) = (b_0+b_1x+\dots+b_kx^k)(c_0+c_1x+\dots+c_hx^h)$

$b_0c_0 = 3$ wlog $3 \mid b_0$ $3 \nmid c_0$

$\underbrace{b_1c_0+b_0c_1}_{} = 0 \Rightarrow 3 \mid b_1$, con $b_0 \uparrow 3$

$b_2c_0+b_1c_1+b_0c_2 \Rightarrow 3 \mid b_2$, con $b_1 \uparrow 3$, $b_0 \uparrow 3$

Questa storia va avanti fino a $3 \mid b_{n-2}$ [formalmente scrivere induzione]

[Oss. Non importa se h e k sono molto più piccoli di $n-2$: posso sempre far finta che i coeff. successivi siano 0]

- Se $\deg(B(x)) \le n-2 \Rightarrow$ MCDC $(B(x))$ è almeno 3, quindi anche MCDC $(A(x))$ deve essere almeno 3. ASSURDO
- Se $\deg(B(x)) = n \Rightarrow$ non è una fattorizzazione $\Rightarrow$ ASSURDO
- Se $\deg(B(x)) = n-1 \Rightarrow \deg C(x) = 1 \Rightarrow C(x) = x-a$ con a radice di $A(x)$ (tutto è monico)

Devo escludere che $A(x)$ abbia radice intera, sarebbe $a=\pm 1$ oppure $a=\pm 3$ e si escludono facilmente. Somma di 3 dispari...

—o—o—

EISENSTEIN GENERALIZZATO $a_0+a_1x+\dots+a_nx^n$

$p^2 \nmid a_0$ $p \mid a_i$ per $i=0,1,\dots,k<n$ $p \nmid a_{k+1}$

Cosa possiamo dedurre? La solita storia va avanti fino al grado k, quindi, se è fattorizzabile, almeno 1 dei fattori ha grado $\ge k+1$.

Sol 2 Riduco in $\mathbb{F}_3[x]$: $x^n+2x^{n-1} = x^{n-1}(x+2) = \bar{A}(x)$

Quindi $B(x) = \underbrace{x^k}_{\bar{B}(x)} + 3Q(x)$ $C(x) = \underbrace{x^{n-1-k}(x+2)}_{\bar{C}(x)} + 3R(x)$

I termini noti sarebbero entrambi multipli di 3, a meno che $k=0$ oppure $k=n-1$

$\boxed{\text{IMO 2002-3}}$ Trovare le coppie (m,n) di interi t.c.

$$\frac{a^m+a-1}{a^n+a^2-1} \in \mathbb{Z} \quad \text{per infiniti valori di } a \in \mathbb{Z}.$$

$\boxed{\text{IDEA 1}}$ Fatto generale : se $\frac{P(x)}{Q(x)}$ è intero per ∞ $x \in \mathbb{Z}$, allora $Q(x) \mid P(x)$

$P(x) \in \mathbb{Z}[x]$, $Q(x) \in \mathbb{Z}[x]$ monico

Dim. $P(x) = Q(x)A(x) + R(x)$

$$\Rightarrow \frac{P(x)}{Q(x)} = \underset{\substack{\uparrow \\ \text{intero sempre}}}{A(x)} + \boxed{\frac{R(x)}{Q(x)}}$$

deve essere intero per ∞ valori di x

Poiché $\deg(Q) > \deg(R)$, allora per $|x|$ abbastanza grandi si ha che

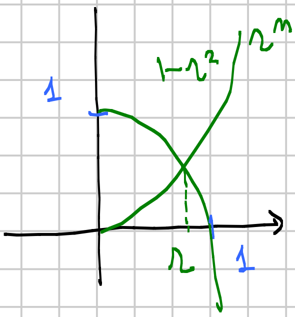
$$|R(x)| < |Q(x)|$$

Questo impedisce a $\frac{R(x)}{Q(x)}$ di essere intero per ∞ valori, a meno che $R(x)$ non faccia 0 per ∞ valori $\Rightarrow R(x) \equiv 0$.

$\boxed{\text{IDEA 2}}$ Se $\overbrace{a^n+a^2-1}^{Q(a)}$ deve dividere $\overbrace{a^m+a-1}^{P(a)}$, tutte le radici del 1° devono essere radici del 2° (anche quelle complesse)

Ora $Q(x)$ ha una radice $r \in (0,1)$ $\qquad Q(0)=-1$, $Q(1)=1$

$r^n+r^2-1=0 \qquad r^n = 1-r^2$



$\boxed{\text{IDEA 3}}$ Durissimo! Se voglio che r sia radice di $P(x)$ deve essere $m<2n$

Supponiamo di averlo dimostrato

$\boxed{\text{IDEA 4}}$ Faccio la divisione di polinomi

$a^n+a^2-1 \mid a^m+a-1$

$a^n+a^2-1 \mid a^m + a^{m-n+2} - a^{m-n}$

Sottraendo ottengo

$a^n+a^2-1 \mid a^{m-n+2} - a^{m-n} - a + 1$

Ma allora $m-n+2 \geq n \Rightarrow m \geq 2n-2$

Restano 2 casi

- $m = 2n-2$ $\qquad a^n + a^2 - 1 \mid a^m - a^{n-2} - a + 1$

$$a^n + a^2 - 1 \mid a^m + a^2 - 1$$

Differenza: $\quad a^n + a^2 - 1 \mid a^{n-2} + a^2 + a - 2 \qquad$ Difficile...

- $m = 2n-1$ $\qquad a^n + a^2 - 1 \mid a^{m+1} - a^{n-1} - a + 1$

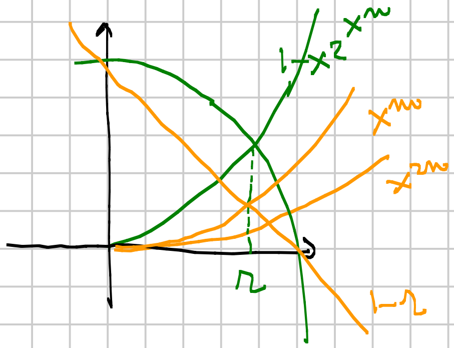
$$a^n + a^2 - 1 \mid a^{m+1} + a^3 - a$$

Differenza: $\quad a^n + a^2 - 1 \mid a^{n-1} + a^3 - 1$

Questo è possibile se il grado a RHS è 3 e $n = 3$ ... e funziona

—o —o —

Resta da capire che se $r^n + r^2 - 1 = 0$ e $r^m + r - 1 = 0$ con $r \in (0,1)$, allora $m < 2n$



Nell'equazione $1-x = x^m$, più m cresce, più la soluzione si sposta verso destra

Per dimostrare che $m < 2n$, basta verificare che per $m = 2n$ l'intersezione è già a dx dell'r precedente

Basta che prenda il valore di r che risolve la 1ª eq. e dim. che

$$1 - r > r^{2n}$$

Ipotesi: $\quad r^n = 1 - r^2$

Tesi: $\quad r^{2n} < 1 - r$

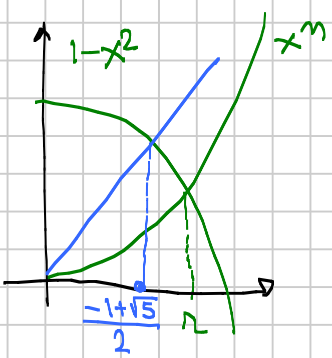
$$(1-r^2)^2 < 1-r$$

$$\cancel{1} - 2r^2 + r^4 < \cancel{1} - r$$

$$r^4 - 2r^2 + r < 0$$

$$r(r^3 - 2r + 1) < 0$$

$$\underset{+}{r}\,\underset{-}{(r-1)}\,\underbrace{(r^2+r-1)}_{\text{deve essere }+} < 0$$



vero se $r > \boxed{\frac{-1+\sqrt{5}}{2}}$ $\quad$ risolve $x = 1 - x^2$

$\boxed{\text{PASSO 1 in modo aritmetico}}$ $\quad a^n + a^2 - 1 \mid a^m + a - 1 \quad m < 2n$

$a = 2 \qquad 2^n + 3 \mid 2^m + 1 \qquad d = 2^n + 3$

$2^m + 1 \equiv 0 \pmod{d} \qquad 2^m \equiv -1 \pmod{d}$

$2^m = 2^n \cdot 2^{m-n} \equiv -3 \cdot 2^{m-n} \equiv -1 \pmod{d}$

$3 \cdot 2^{m-n} \equiv 1 \pmod{d} \qquad d = 2^n + 3$

Se fosse $m \leq 2n-2$, avremmo che $\quad 1 < 3 \cdot 2^{m-n} \leq 3 \cdot 2^{n-2} < d$
e non può essere perché è congruo ad 1

Se fosse $m = 2n-1$, avremmo che $\quad 1 < 3 \cdot 2^{m-n} = 3 \cdot 2^{n-1} < 2d$

Quindi $\quad 3 \cdot 2^{n-1} = d + 1 = 2^n + 4 \qquad 3 \cdot 2^{n-1} = 2 \cdot 2^{n-1} + 4$

$2^{n-1} = 4 \Rightarrow n = 3.$